Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1725 07/10/15

~ 'Hacking Team' Hacked! ~ People Are Talking! ~ New Atari Comics?
~ First Look at Firebee! ~ Major Firefox Patches! ~ PSN Hacker Guilty!
~ Win 10 Almost A Wrap! ~ Student Writes Malware ~ Chrome Tops Firefox

~ Google Search Poisoned ~ Windoes 8.1 Passes XP! ~ DuckDuckGo Soars!

-* Nintendo’s PlayStation Found *-
-* Hillary: China Hacks Everything..." *-
-* Cybersquatters & Presidential Candidates! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

It’s been another long week, and yet another "late" issue - I apologize. But, I’m sure that it will all be worth the wait! Lots of interesting stuff this week, including thew beginning of what should be an informative discussion by Fred Horvat on his new Firebee acquisition. Be sure to stay tuned for his observations and experiences!

The summer is starting to take hold here in New England, but we’ve been fortunate so far not to have been hit with scorching temperatures. We haven’t been hit with a 90-degree day yet - a plus as far as I’m concerned. We’ve had some rain, resulting in some closer-to-normal drought conditions. That’s always a good thing!

Well, enough of the small talk - let’s get right to the good stuff!

Until next time...

=~=~=~=

Checking Out The Firebee!

I ordered a Firebee for my 50th Birthday and it arrived today! So far the 30 minutes I messed with it has not gone so well. Right now it appears the CF Card has either come loose or more likely got corrupted. It’s not obvious how to open the unit to get to the CF card to check so I emailed Mathias about opening the case or for other suggestions.

Not so good at the moment. (Dana this will make a decent weekly contribution to AONE. I will have to start something next week if I don’t write something tonight or tomorrow for you.)

It appears that the Compact Flash drive is corrupt. Which is both good and bad but mostly bad.

Bad - Because I can’t use my new expensive toy.
Good - Because I have to lean how the machine works and have to install MiNT from scratch.

Biggest problem for me or anybody else getting one of these who did not

follow or develop for/on a Firebee the last few years is that almost everything about it is assumed that you know everything about the Firebee inside and out before turning it on. What you know about you Atari ST helps but this is a completely different beast in every way.

You know you are in for a wild ride when you read the Quick Start from Fredi at Medusa thanking you for purchasing an Alpha Product. So the next revision they are working on will hopefully correct a lot of bugs and non function hardware on the board. I will be in contact with the ACP team in updating the documentation and mostly creating documentation so that a noob doesn't have to go through what I am.

For example on documentation in installing MiNT. One of the first steps says Prepare CF Card. OK great HOW? I'm staring at a TOS Desktop and how do I do that? So that's one of the items I want to update. What got me was the Video Resolution Test. I got some real nasty looking horizontal lines. I thought the monitor was not capable so I got another monitor. When in fact this meant the monitor was good. The documentation never mentions this. After the fact I looked online and others complained about this on Atari-Forum.com also.

Stay tuned for regular updates!

=~=~=~=

->In This Week's Gaming Section - PSN & Xbox Live Hacker Guilty!
"""""""""""""""""""""""""""""""" Nintendo's PlayStation Found!
Dynamite and Atari Team Up for New Comic Vent
ures!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Lizard Squad Member Found Guilty of Hacking Into PlayStation Network and Xbox Live

Julius "zeekill" Kivimaki, one of the members of Lizard Squad - the gang of hackers infamous for launching a distributed denial-of-service attack on PlayStation Network (PSN) and Xbox Live gaming services around Christmas last year - has been found guilty of 50,700 offences related to computer crimes in Finland according to Finnish newspaper Kaleva.

Kivimaki played an integral role in last year's attacks and was also the group's spokesman in on-air interviews with Sky News. In order to bring down PSN and Xbox Live, the group used thousands of hacked home Internet routers.

However, Kivimaki will not being going to jail. Rather, he has received a two-year suspended prison sentence and his Internet activity will be monitored by the Finnish police.

While a large chunk of the Internet is up in arms due to the leniency of the sentence, the Lizard Squad Twitter account was having a field day, gloating about getting away scot-free in a string of tweets, one of which reads: "All the people that said we would rot in prison don’t want to comprehend what we’ve been saying since the beginning, we have free passes."

Another tweet read ruled out extradition, saying: "And no zeekill will not be extradited. Finnish citizens have the right to refuse extradition regardless of any treaty."

Nintendo’s PlayStation, The Holy Grail of Game Memorabilia, Has Been Found

An extraordinarily rare prototype of the Nintendo PlayStation console, which was created as part of a failed partnership between Nintendo and Sony some 25 years ago, has been discovered.

Never-before-seen images offer the first ever close-ups of the machine, now yellowed with age, which combines the form factor of the SNES along with the branding of PlayStation.??When it was first revealed in 1991, the system was referred to as the "Nintendo Play Station", and Sony was thought to have created some 200 prototypes. The pitch from the electronics giant was that the console would not only play Nintendo game cartridges but also games on compact disks. However, due to a public fall-out between both companies, the prototypes were destroyed.

However, one unit appears to have survived. This unit is so rare that its specific design features, such as a horizontal volume slider at the front and an assortment of outputs at the back, were not public knowledge.

The console is historically significant because it represents the brief partnership between Nintendo and Sony prior to its intense rivalry that still exists today.

At the Consumer Electronics Show in 1991, Sony showcased its Nintendo-endorsed vision for a SNES-CD, which it branded with a "PlayStation" logo. Nintendo shocked Sony, however, by suddenly announcing - at the same show - that it would be partnering with electronics firm Phillips instead.

Incensed and embarrassed, the Sony executive Ken Kutaragi began to internally lobby the company to fund plans to build a console without Nintendo’s support. The outcome of that plan, also called the PlayStation, brought about a tectonic power-shift in the games business.

This prototype model was found by the son of a businessman who had ties with a former Sony executive, believed to be Olafur Olafsson, who was the chief executive of Sony Interactive Entertainment in 1991.

The son, who is only known by his online handle ’Dnldbld’, first published the images on Reddit, and then on Assembler Games. He says that he will try to find the power supply for the prototype and boot the system up for

the first time.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Dynamite and Atari Team Up for New Comic Ventures

Dynamite Entertainment announced that it will team up with Atari, Inc. in a collaboration that will include securing the rights to a retrospective hardcover book comprised of photos and concept artwork, as well as behind-the-scenes information and interviews with those involved in Atari s history. The collaboration allows the company to publish original graphic novels and comics based on popular Atari properties such as Asteroids, Centipede, Missile Command, Crystal Castles and Tempest. In addition, Dynamite plans to re-print existing material such as the 1980s Atari Force comics.

'Atari' doc trailer digs deep into legend of infamous 'E.T.' video game
We are excited to be teaming up with Dynamite Entertainment to bring a modern twist to a classic series of comics and table top books that are rich with historic art, Fred Chesnais, Chief Executive Officer of Atari said in a statement. Atari s roots in the comic book world and iconic art is a collector and video game enthusiast s dream. Our partnership is a fun way to expose our brand to a new generation and resonate with our long-time fans.

Atari is a touchstone for so many people, added Dynamite Director of Business Development Rich Young. Their games and game system exposed a lot of folks to video games for the first time and frankly, got them hooked! I have fond memories of playing games on the 2600 with friends growing up, and am quite happy that we have a chance to work with Atari on this publishing program.

Originally founded in 1972, Atari was the pioneer of video consoles and arcade games, and helped pave the way for the entertainment gaming industry throughout the next decade. Dynamite s products will be available through comic book stores and digital platforms such as Comixology and Dynamite Digital.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Hillary Clinton: China Hacks ’Everything That Doesn’t Move’ in the US

US presidential hopeful Hillary Clinton has accused China of state-sponsored hacking designed to steal both trade secrets and government information.

Speaking at a Fourth of July campaign rally in New Hampshire on Saturday, the former US Secretary of State said the rise of China was the story of the 21st century and how the US responded to that would determine the future of the entire world.

She added that she hoped to see China prosper in a peaceful way but also warned that vigilance was required.

The US has to be aware, she said, that China’s military strength is increasing quickly as the nation continues to establish new military installations in contested territories - such as the Philippines - and other countries the US has treaties with.

Scrawling her foreign policy credentials on the cyber blackboard, she said: They’re also trying to hack into everything that doesn’t move in America. Stealing commercial secrets, blueprints... from defense contractors, stealing huge amounts of government information, all looking for an advantage.

Make no mistake: they know they’re in a competition, and they’re going to do everything they can to win it.

Quite what Clinton means by "everything that doesn’t move" is not clear. After all, we know that most assets compromised by a hack or error certainly do move. And I’m not just talking about mechanical devices such as aeroplanes, drones or even cars; there are other, more personal targets too: us.

Fortunately, the effects of hacking are now being taken far more seriously by court systems that are beginning to appreciate the effects of a crime that doesn’t involve actual or threatened physical violence against property or the person.

Take for instance the case of Alex Yucel, the co-creator of the Blackshades RAT. He was recently sentenced to 57 months in jail over the malware that had the capability to steal banking and other information, as well as hold machines to ransom or use their computing power as part of a DDoS network - a win for the good guys, as John Shier said to Paul Ducklin in the latest Chet Chat podcast (from 8m 24s).

Hillary Clinton’s comments come three months after a huge breach at the US Office of Personnel Management left the personal records of millions of federal employees compromised. US officials said at the time that they believed China was behind the attack which bore a striking resemblance to a similar incident the previous year.

China, as to be expected, denied all claims of wrongdoing.

Of course it’s not the first time that the US has accused China of nation-state hacking, nor is it the first time that Clinton herself has wagged her finger in that direction.

In 2010 she demanded an explanation from China after Google claimed it had

experienced a "highly-sophisticated" attack that led to the theft of intellectual property. Subsequently named "Operation Aurora," the attack also impacted a large number of other US financial and technology companies as well as military organisations.

Unsurprisingly, the finger pointing goes both ways - the Chinese government has recently been able to cite Edward Snowden’s revelations as proof that the US has launched cyber attacks in the other direction.

I wonder what a possibly-future President Clinton would have to say about that?

Hacking Team Spyware Company Hacked, Embarrassing Emails Revealed

Hacking Team, a company that helps police hack citizens, has been hacked itself. In a series of tweets from the company s compromised Twitter account, the unknown hackers appear to have revealed embarrassing internal emails and a torrent with 400GB of internal files, source code, and communications. One particular tweet appears to show an email from Hacking Team CEO David Vincenzetti, mocking a competitor for being severely hacked. No hacking groups have claimed responsibility for the breach yet.

Hacking Team has more than 40 employees and sells commercial hacking software to law enforcement in several dozen countries, including Morocco, Ethiopia, and the United Arab Emirates. A recent report from Motherboard revealed that the Hacking Team also supplies spyware tools to the Drug Enforcement Agency to implant software in a suspect s phone and record texts, emails, passwords, and monitor conversations.

Hacking Team is infamous in security circles for injecting targeted malware into YouTube and Microsoft s Live services. Formed by two Italian programmers, the pair originally created a program called Ettercap that quickly became the weapon of choice for hackers wanting to spy on people. The success of Ettercap led to Hacking Team, and now attention from rival hackers who have renamed the company s Twitter account to Hacked Team.

Hacking Team Breach Shows a Global Spying Firm Run Amok

Few news events can unleash more schadenfreude within the security community than watching a notorious firm of hackers-for-hire become a hack target themselves. In the case of the freshly disemboweled Italian surveillance firm Hacking Team, the company may also serve as a dark example of a global surveillance industry that often sells to any government willing to pay, with little regard for that regime s human rights record.

On Sunday night, unidentified hackers published a massive, 400 gigabyte trove on bittorrent of internal documents from the Milan-based Hacking Team, a firm long accused of unethical sales of tools that help governments break into target computers and phones. The breached trove includes executive emails, customer invoices and even source code; the company s twitter feed was hacked, controlled by the intruders for nearly 12 hours, and used to distribute samples of the company s hacked files.

The security community spent Sunday night picking through the spy firm s innards and in some cases finding what appear to be new confirmations that Hacking Team sold digital intrusion tools to authoritarian regimes. Those revelations may be well timed to influence an ongoing U.S. policy debate over how to control spying software, with a deadline for public debate on new regulations coming this month.

One document pulled from the breached files, for instance, appears to be a list of Hacking Team customers along with the length of their contracts. These customers include Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Morocco, Nigeria, Oman, Saudi Arabia, Sudan, and several United States agencies including the DEA, FBI and Department of Defense. Other documents show that Hacking Team issued an invoice for $1 million to Ethiopia s Information Network Security Agency (the spy agency of a country known to surveil and censor its journalists and political dissidents) for licensing its Remote Control System, a spyware tool. For Sudan, a country that s the subject of a UN embargo, the documents show a $480,000 invoice to its National Intelligence and Security Services for the same software.

These are the equivalents of the Edward Snowden leaks for the surveillance industry, says Eric King, the deputy director of Privacy International. There are few countries [Hacking Team] aren t willing to sell to. There are few lines they aren t willing to cross.

In its marketing materials, Hacking Team describes its RCS product as a solution designed to evade encryption by means of an agent directly installed on the device an agency is monitoring. You want to look through your target s eyes, reads the script of one of the company s videos, shown below. You have to hack your target. Last year, researchers at Toronto-based Internet surveillance analysis group Citizen Lab and antivirus firm Kaspersky revealed Hacking Team software that targets every mobile operating system to take total control over phones.

Hacking Team hasn t yet responded to WIRED s request for comment. One Hacking Team engineer, Christian Pozzi, seemed to defend his employer briefly on Twitter, writing that the company s attackers were spreading lies about the services we provide. His feed was soon hacked and then deleted.

Hacking Team s newly exposed business practices call into question whether current regulations effectively prevent a private firm from selling hacking software to any government in the world. One written exchange between Hacking Team s executives and UN officials shows the UN questioning Hacking Team s sales to Sudan. A letter from the UN to the company references a March 2015 letter Hacking Team sent the UN, in which it argued that its spying tools didn t count as a weapon, and so didn t fall under the UN s arms embargo. (The UN disagreed.)

Sudan is one of the most strictly embargoed countries in the world, says Chris Soghoian, a privacy activist and lead technologist for the American Civil Liberties Union who first spotted the UN correspondence in the Hacking Team data dump. If Hacking Team believes they can lawfully sell to Sudan, they believe they can sell to anyone.

That issue of whether hacking tools are defined as weapons in the terms of arms control agreements couldn t be more timely: An arms control pact called the Wassenaar Arrangement has been hotly debated in recent weeks over its measures that would control the international export of intrusion software. The US Department of Commerce has opened the process to public comment, a window that ends on July 20.

The Wassenaar Arrangement has been criticized by the hacker community as limiting security research and preventing the sharing of penetration testing tools. But Privacy International s Eric King argues that the practices of Hacking Team demonstrate why the pact is necessary, along with what he describes as carve-outs to protect security research. What s clear is that these companies can t be left to their own devices, says King. Some form of regulation is needed to prevent these companies from selling to human rights abusers. That s a hard policy question, and one tool won t be a silver bullet. But regulation and export controls should be part of the policy response.

The issue of whether hacking tools are defined as weapons in the terms of arms control agreements couldn’t be more timely.

Despite Hacking Team being based in Italy, the US Department of Commerce s still-evolving export control regulations may still apply to the company, says the ACLU s Chris Soghoian. He points to two firms he spotted in Hacking Team s breached files who appeared to be reselling the company s tools: Cyber Point International in Maryland and Horizon Global Group in California.

The hacked documents are far from the first evidence that Hacking Team has sold its tools to authoritarian governments. Researchers at Citizen Lab have accused Hacking Team of selling to countries including Sudan and the United Arab Emirates, who used it to spy on a political dissident who was later beaten by thugs. WIRED reported in 2013 on an American activist who was apparently targeted by Turkey using Hacking Team tools. But Hacking Team has responded with denials, criticisms of Citizen Lab s methods, and claims that it doesn t sell to repressive regimes.

 Hacking Team has continuously thrown mud, obfuscated, tried to confuse the truth, says Privacy International s King. This release helps set the record straight on that, and shows their deviousness and duplicity in responding to what are legitimate criticisms.

Cybersquatters Giving Some US Presidential Candidates A Bad Name

Chris Christie, the governor of New Jersey, is about to announce he’s running to become the next president of the United States - something he alluded to this past weekend when he began tweeting out links to his website, chrischristie.com.

But first, Governor Christie needed to secure the website domain from its previous owner, a computer programmer from Wisconsin with the same name.

It’s not clear how the politician Christie acquired the domain from the programmer Christie (we’ve contacted the latter to inquire about it, but haven’t heard back) - but it might have cost the governor a substantial sum of money to acquire it.

Another candidate for president, Senator Rand Paul, reportedly paid a group of his own supporters who owned of randpaul.com $100,000 for that domain.

In the cases of chrischristie.com and randpaul.com, the former domain owners were acting in good faith, rather than registering those websites

merely for the purpose of getting the high-profile politicians to purchase the domains.

On the other hand, the owner of chrischristie2016.org registered that domain back in 2011 in hopes that Christie would be running for office in 2016 and offer to buy it.

Registering a domain in good faith is an important distinction, because buying up domains with names of famous people or brands for the purpose of extorting money is what is known as cybersquatting, and it’s (supposed to be) illegal.

The Anticybersquatting Consumer Protection Act (ACPA) is intended to prevent cybersquatting for profit.

Corporations like Facebook and Pinterest have successfully sued cybersquatters who registered domains that were close to the correct domains but were off by a letter or two, like facegbook.com or pimterest.com, taking advantage of people who inadvertently mistype the web address.

This kind of abuse is what Sophos calls "typosquatting" - and it’s not just a nuisance, but possibly dangerous for web users who accidentally visit those websites.

A few years ago, we conducted an experiment where we surveyed 1500 websites with one-character mistakes in the web addresses of six well-known domains - for Facebook, Google, Twitter, Microsoft, Apple and, while we were at it, Sophos.

We discovered that about 3% of those misspelled websites were associated with phishing, spam, and other types of cybercrime.

But disputes over domain names, and whether a domain owner is acting in "bad faith," aren’t always cut and dry.

The ACPA law allows people to register domains for purposes that include political speech, which can lead to some embarrassing or reputation-damaging websites registered by political opponents.

Senator Ted Cruz, a presidential candidate and staunch opponent of President Obama’s immigration policies, doesn’t own tedcruz.com - it’s instead owned by someone using the site to host the message: "Support President Obama! Immigration Reform Now!"

Carly Fiorina, the former chief executive of HP who is now running for president, didn’t register carlyfiorina.org, and that website now hosts a message highlighting the fact that Fiorina laid off 30,000 HP workers during her tenure.

And the owners of the domain JebBushforPresident.com aren’t supporters of presidential candidate Jeb Bush - they purchased the domain in 2008 in response to Bush’s "horrible record with regards to LGBTQ rights," they said.

According to the Internet Corporation for Assigned Names and Numbers (ICANN) - the non-profit organization responsible for managing the top-level domain name system and Internet Protocol (IP) allocation - if you believe someone has registered your trademarked name in bad faith, you can file a complaint under the Uniform Domain-Name Dispute Resolution

Policy.

You could also file a lawsuit against the domain owner, which real estate mogul and now presidential candidate Donald Trump did in 2014 in response to a squatter who registered several websites using Trump’s name.

Trump won the lawsuit, which resulted in a judgment that the squatter would have to pay Trump $32,000 in damages.

But not every business or individual has Trump’s resources for fighting off squatters with lawsuits, and defending against cybersquatting by registering all potential domains containing your name or trademark is an expensive proposition.
ICANN has begun approving a set of 600 new generic top-level domains (gTLD), including the potentially embarrassing .SUCKS and .XXX.

According to the Coalition Against Domain Name Abuse, trademark owners who want to pay to block registration of their names across 300 new gTLDs during the pre-registration period could pay as much as $330,000 to protect their brands from cybersquatters.

In addition to the costs to businesses, the CADNA notes that cybersquatting potentially exposes consumers to counterfeit goods, fraud, malicious websites and identity theft.

The CADNA has proposed changes to the ACPA law that it hopes will be deterrents against future abuse of the domain name system - raising penalties for violators and holding domain registrars accountable.

In the meantime, brand owners can make cybersquatting less profitable by refusing to pay squatters for domains; and consumers can avoid potentially harmful domains and avoid typosquatting sites by bookmarking their favorite websites or using search engines to find the most relevant website.

As for the 2016 presidential candidates, it might be time to start buying up domains in preparation for another run in 2020.

Standoff Over Social Media Passwords Breaks New Legal Ground

A Texas man used social media to promote his gun store, posting politically charged messages that criticized the president and promoted Second Amendment rights.

But after losing ownership of his suburban Houston store in bankruptcy, Jeremy Alcede spent nearly seven weeks in jail for refusing a federal judge’s order to share with the new owner the passwords of the business’ Facebook and Twitter accounts, which the judge had declared property.

"It’s all about silencing my voice," said Alcede, who was released in May after turning over the information. "... Any 3-year-old can look at this and tell this is my Facebook account and not the company’s."

Alcede’s ultimately failed stand charts new territory in awarding property in bankruptcy proceedings and points to the growing importance of social media accounts as business assets. Legal experts say it also provides a lesson for all business owners who are active on social media.

"If your business is something you feel very passionately about, it can be hard to separate those things," said Benjamin Stewart, a Dallas-based bankruptcy lawyer. "The moral for people is you have to keep your personal life separate from your business life."

U.S. Bankruptcy Judge Jeff Bohm, who handled Alcede's case, acknowledged "the landscape of social media is yet mostly uncharted in bankruptcy," and cited a 2011 New York bankruptcy court case that treated such accounts like subscriber lists, which "provide valuable access to customers and potential customers."

Other cases in the U.S. and abroad have touched on similar issues. In 2012, a South Carolina Internet company settled a lawsuit filed against a former employee it had said cost them thousands of dollars in lost business when he took 17,000 Twitter followers with him. A Pennsylvania federal court in 2013 ruled in favor of a woman who had sued after her former employer took over her LinkedIn account following her firing.

That same year, a British court approved a company's request to temporarily stop a group of ex-employees from using the firm's LinkedIn contacts to start a rival business. The employees claimed the LinkedIn accounts and contacts were personal.

Villanova University School of Law professor Michael Risch said Facebook and Twitter accounts, among other social media platforms, are now seen as property by companies.

"I suspect that's what the judge was looking at, is this primarily an asset being used for business advertising to get customers to talk about what is going on with the company," said Risch, who specializes in Internet law. "It might have started out as a personal (account) but turned into a business property."

Alcede, however, remains defiant, even after his release from jail, saying his refusal to hand over the passwords was not about keeping his Facebook page but fighting tyrannical big government.

He said his Facebook posts and tweets criticizing President Barack Obama and supporting gun owners' rights were his personal views and not done to promote the business. But Bohm ruled in April that the gun store's social media accounts were not personal but used to boost sales, citing a tweet in which Alcede told his followers he was at a gun trade show as an example of something that would attract customers because it showed him as a "connected insider in the gun-buying community."

Control of the store and social media accounts was given to Steven Coe Wilson, Alcede's former business partner. Bohm's ruling described Alcede as a "disgruntled former business partner" trying to control assets that no longer belonged to him.

Alcede, who in June filed a motion to revoke the bankruptcy plan, had argued the accounts weren't listed as assets in the bankruptcy court filings. He told The Associated Press he only turned over the passwords so he could deal with various personal issues, including health problems he developed while jailed.

Wilson said in an email he couldn't comment until Bohm releases the company from bankruptcy. Richard Kincheloe, Wilson's attorney, did not return phone calls seeking comment, but said at an April court hearing that the issues

related to the social media accounts were "not about what someone is allowed to say. It’s about paying creditors."

If the new owners could not access the business’ accounts and send messages to followers, it could impact the store’s profits, making it less valuable, Stewart said. While having Alcede spend seven weeks in jail over the passwords was "harsh," Stewart said that in the end, Alcede held the key to his freedom.

"You have to strike a balance between making sure people respect the court’s authority and giving people the right to make their own decision and accept the consequences if that is the way they want to go," he said.

Mystery Vandals Are Cutting Fiber-optic Cables in California

Somebody is cutting underground fiber-optic cables in Northern California.

The FBI said last month that it was investigating a rash of cable-cutting vandalism in the San Francisco Bay Area - 10 incidents over the past year - that resulted in loss of internet and phone service.

On Tuesday, 30 June, the 11th such case of vandalism cut off service for customers of Wave Broadband, near the state capital of Sacramento, which the internet service provider said was the result of a widespread "coordinated attack."

Not so, according to the FBI, instead saying the most recent incident was confined to one area and not part of a coordinated attack.

The FBI branch in San Francisco also said there is "no indication these incidents are linked" to a case of vandalism in April 2013 that local law enforcement officials called "sabotage," where a suspect cut fiber-optic cables, knocking out 911 service, and then fired a rifle at a PG&E power substation.

On the other hand, the 11 recent cases of cable-cutting do have enough similarities to make you wonder if they are related.

According to a report in USA Today, many of the incidents involved breaking into underground vaults to cut multiple cables, which would have required special equipment to enter the vaults and cut through protective sheathing on the cables.

The cables cut on Tuesday belong to Level 3 Communications and Zayo Group Holdings, two companies that own network "backbones," which ISPs, cable and phone companies use to connect to the internet.

It took about five hours on Tuesday for the companies to fix the cables and restore service, but the FBI’s presence on the scene for its investigation slowed the repair efforts, according to the Wall Street Journal.

It’s not known how many customers lost service, but one big customer - Microsoft - reported on Tuesday that its Azure cloud service experienced "intermittent connectivity issues" in the Western and South Central US due to "fiber cuts in the Western US."

FBI Special Agent Greg Wuthrich told USA Today that the vandalism was "disturbing," and asked the public to come forward with tips:

When it affects multiple companies and cities, it does become disturbing. We definitely need the public’s assistance.

The individuals responsible may appear to be "normal telecommunications workers," or have special equipment related to that job, the FBI said.

Yet the FBI is at a loss to explain the cable-cutting incidents of the past year and knows of "no real motive," Ars Technica reported.

Just how vulnerable is the internet to this kind of sabotage?

The fiber-optic cables that carry the majority of the internet’s traffic are basically bundles of thin strands of glass that transmit data that is converted into light at one end of the cable and then converted back into data at the other end.

Cables are usually buried only a few feet underground and are small enough around - about the size of a finger - to be cut with scissors.

The California incidents impacted customers in multiple cities at a time, but it’s possible to knock out internet service to a much wider area with little more than a shovel.

In 2011, we reported on an incident that knocked out service to 90% of Armenia when a 75-year-old woman from Georgia struck a cable while digging for copper to sell.

To travel longer distances, internet traffic is carried by large undersea cables that are also vulnerable to accidental severing - by ship anchors or even shark bites.

In 2008, two major undersea cables were cut leading to widespread internet and phone outages across the Middle East - leading some to speculate that it was deliberate attack.

Losing internet service, even for a few hours, can cause big disruptions with big consequences.

Usually, when we think of the security of the internet we worry about defending against cyberattacks that could knock out financial, industrial, government or military networks.

We should also be thinking about how to protect the internet from physical attacks on its infrastructure.

This 20-year-old Student Has Written 100 Malware Programs in Two Years

Security firm Trend Micro has identified a 20-year-old Brazilian college student responsible for developing and distributing over 100 Banking Trojans selling each for around US$300.

Known online as ’Lordfenix’, ’Hacker’s Son’ and ’Filho de Hacker’, the computer science student first began his career by posting in forums, asking for programming help for a Trojan he was developing, researchers

said.

However, Lordfenix has "grown quite confident in his skills" and began developing and distributing malware tailored to pilfer financial information since at least 2013.

"Based on our research, Lordfenix has created more than 100 different banking Trojans, not including his other malicious tools, since April 2013," Trend Micro says. "With each Trojan costing around R$1,000 (roughly $320), this young cybercriminal channeled his talent in programming into a lucrative, illegal venture."

Trend Micro has also provided an image of the hacker’s Facebook wall post (given below) in which the hacker shows a considerable amount of local currency.

In order to expand his operation, Lordfenix has now begun offering free versions of fully-functional Banking Trojan source code other wanna-be cyber criminals on the underground forum.

The free versions of the Trojan can be used to steal login details from customers of four different Brazilian banking websites including HSBC Brazil, Bank of Brazil, and Caixa. For access to other financial institutions, ’clients’ have to pay for a more powerful tool, TSPY_BANKER.NJH.

TSPY_BANKER.NJH is a Trojan capable to identify when a user enters any of a target bank’s URLs into their browser. The malware then shuts down the browser window (if it is running on Google Chrome), displays an error message, and then opens a fake Chrome window.

Once the victim enters the login details into the fake window, the information is sent back to the attackers address via email.

As an extra precaution, Lordfenix’s malware also includes a software program to terminate a security process called GbpSV.exe, which is used by large number of Brazilian banks in an effort to keep their online customer data secure.

Malware Threat to Online Banking is Growing rapidly and countries like Brazil, where almost half of all financial transactions are conducted online, have come up as a boon for hackers.

Privacy Outcry Over Proposal To Reveal Website Owners’ Identities

People fighting for their privacy rights are deluging domain overseer ICANN with comments opposing a proposal that would strip the rights of commercial domains to use proxy services to shield registrants’ true identities and addresses.

It might seem like a straightforward issue of prohibiting proxy use by domains "actively used for commercial transactions," but it’s not that easy, as dissenting members of ICANN pointed out.

In ICANN’s report on the issue of privacy/proxy service accreditation, the members said the move could work against persecuted groups and organizations, including minority political groups or those devoted to

gender orientation:

[M]embers of the [working group] noted that fundraising and membership drives are often performed by the very groups and organizations seeking privacy/proxy registration for protection, including minority political groups, minority religious organizations, ethnic groups, organizations committed to change of racial policies, gender orientation groups, and publications engaged in freedom of expression. These groups and their representatives note that, in the laws of their countries, the mere collection of a donation or membership fee does not change their status from "non-commercial" to commercial. Others noted that "non-profit" status is limited to only a few countries.

The Electronic Frontier Foundation (EFF) focused on the issue on Tuesday, with a post that detailed how the change is being pushed by US entertainment companies that told Congress in March that privacy for domain registration should be severely restricted.

Such companies want ever more names and contact information in their zeal to accuse people of copyright and trademark infringement, preferably without having to bother with getting a court order, the EFF said.

The typical number of responses ICANN receives in its public comment periods hovers around 20, according to The Register.

In contrast, the idea of forcing commercial domains to reveal registrants' names and addresses had garnered over 6000 commenters who overwhelmingly opposed the plan as of Thursday morning.

A sample from the comments, from Opus:

With identity theft getting worse by the day, it is imperative that we be able to keep our personal information private. I don't even use my domain email in all instances (including this). I am a single woman living alone and don't want everyone in the world to see where I live. Don't use [F]acebook for the same reason. With just cause, get the [information] needed by taking the legal route.

From Bob Baffy:

I've had issues in the past with people who have abused my personal information through WHOIS searches, and it upsets me that my and other's rights to privacy could be abused again in this way.

The vast majority of comments are coming from people who used form letters supplied by two sites that are campaigning against the change: RespectOurPrivacy.com and SaveDomainPrivacy.org.

A sample of one of the form letters:

Dear ICANN, Regarding the proposed rules governing companies that provide WHOIS privacy services (as set forth in the Privacy and Policy Services Accreditation Issues Policy document): I urge you to respect internet users' rights to privacy and due process. - Everyone deserves the right to privacy. - No one's personal information should be revealed without a court order, regardless of whether the request comes from a private individual or law enforcement agency. Private information should be kept private. Thank you.

The 98-page report focuses on other changes, but it's a dense, wonkish

read, and nothing’s gotten the same level of attention as this issue of denying proxy/privacy services to "commercial" domains.

The EFF’s Jeremy Malcolm and Mitch Stoltz pointed out that subpoenas do just fine in getting website owners’ identities, and we don’t need another mechanism to do so - particularly when the cost/benefit ratio is so unconvincing:

The limited value of this change is manifestly outweighed by the risks to website owners who will suffer a higher risk of harassment, intimidation and identity theft. The ability to speak anonymously protects people with unpopular or marginalized opinions, allowing them to speak and be heard without fear of harm. It also protects whistleblowers who expose crime, waste, and corruption. That’s why EFF opposes the new proposal to roll back anonymity.

Windows 8.1 Finally Edges Past XP on the Desktop

Almost two years after its release, Windows 8.1 has finally surpassed XP in the desktop OS market.

Looking at Web traffic among desktop operating systems for the month of June, Web tracker Net Applications pegged Windows 8.1 at a 13.1 percent share, up slightly from 12.8 percent in May. Over the same time, XP’s share plummeted to 11.9 percent from 14.6 percent the previous month.

No. 1 Windows 7 also grabbed more fans as its share of Web traffic rose to 60.9 percent last month from 57.7 percent in May. And still in fifth place behind Apple’s OS X Yosemite was Windows 8, which saw its share dip down to 2.9 percent from 3.5 percent.

Much of this activity may just be part of the natural chain of events. Over the past several months, Windows 7 and 8.1 have gained a greater chunk of Web traffic as tracked by Net Application, while XP and Windows 8 have lost share. But there may be another factor involved. Due to launch July 29, the next-generation Windows 10 will bring free upgrades for the first year, but only for users of Windows 7 and 8.1. If you’re still running Windows XP or Vista, you’ll have to pay for the new operating system. (Windows 8 users can freely upgrade to 8.1, so that’s a no-brainer.) People who want that free upgrade may be jumping to Windows 7 or 8.1 in order to snag the freebie starting the end of this month.

Windows 10 itself has been available as a technical preview since last October. As such, it still registers as just a blip on Net Applications’ radar. For June, Windows 10’s share of Web traffic was 0.16 percent, up slightly from 0.13 percent the previous month. July’s figures are likely to also show a modest gain. But if enough users bite into Microsoft’s free upgrade offer, August’s numbers for Window 10 should show a significant increase.

Microsoft is counting on Windows 10 to win over many of the people turned off by Windows 8, especially among the desktop and laptop crowd. To lure in PC users, the latest version of Microsoft’s venerable operating system has brought back the Start menu and tweaked Windows apps so you can run them from the desktop in any size window, just as you can a regular desktop application. Microsoft has also positioned Windows 10 as the

unifying software for PCs, tablets and mobile phones, hoping that more people will buy into the entire ecosystem.

Of course, Windows still dominates the operating-system landscape. For June, Windows' overall share of Web traffic was 90.8 percent, according to Net Applications, down a smidgen from 91 percent in May. But that still left Mac OS X with just a 7.5 percent share and Linux with only 1.6 percent.

Microsoft Is Just Days Away From Wrapping Up Windows 10

Microsoft will wrap up work on Windows 10 this week in preparation for distributing the operating system to device makers, according to numerous online reports.

The Redmond, Wash. company will declare Windows 10's "release to manufacturing" (RTM) milestone this week, The Verge contended today.

RTM is a historical way post in Microsoft's development schedule that denotes when code is sufficiently stable to deliver to OEMs (original equipment manufacturers), who use the build to pre-load the OS onto their new devices prior to sale.

Neowin also chimed in today, claiming that "internal sources" indicated Microsoft would sign off on RTM this week.

Others had also found signals of the impending RTM in a recently-leaked edition, pegged as build 10163. Perennial leaker WZor, for example, pointed out that build 10163 included a reference in the OS's Calendar app to Thursday, July 9, as the "RTM Sign-Off" date, when Microsoft is to green light the code as fit.

The BuildFeed website also noted that 10163 was tagged as from "th1," purportedly a reference to the internal RTM branch of "Threshold," a former code name for Windows 10. Another build marked as th1 - 10176 - was issued Sunday by Microsoft, according to BuildFeed.

The last official Windows 10 build was 10162, pushed to testers on July 2. Build 10162 was the third issued within a week, Microsoft's fastest pace yet, another sign that the company was closing on final code.

RTM has lost some of its importance with Windows 10, which Microsoft plans to update and refresh regularly, but device makers have to start somewhere. OEMs armed with the code have a shot at making the lucrative back-to-school sales season in the U.S., contrary to expectations two months ago.

In the past, Microsoft has given OEMs months of lead time. For Windows 8, there was a 12-week lag between RTM and the first devices going on sale with the new OS; Windows 7's grace was 13 weeks. If the recent signs of impending RTM are accurate, Microsoft has pared that to less than three with Windows 10.

But Microsoft's radical development changes mean that it will keep churning out preview builds post-RTM. What remains unclear is what RTM means to Microsoft beyond serving as the build it delivers to OEMs and perhaps retailers, who need the OS to provide upgrade services to

customers who recently purchased Windows 8.1-powered devices.

While Microsoft has said that it will stagger ready-to-upgrade notifications to customers, those alerts will show up only after the company has pushed the file(s) to eligible Windows 7 and Windows 8.1 devices. It could conceivably begin distributing the code in the background beginning this week if it does, in fact, declare RTM, then trigger the upgrade notifications to more than just the Windows Insider testers on July 29.

However, that’s apparently not the plan. "Each day of the roll-out, we will listen, learn and update the experience for all Windows 10 users," said Terry Myerson, who leads Microsoft’s OS and devices groups, last week. Myerson’s comments hinted that Microsoft will not only stick to its "waves" distribution scheme, but push different bits to users over time.

If Microsoft blesses Windows 10 RTM on Thursday, OEMs that sell build-to-order PCs through their online outlets have the best chance of having machines ready by the end of the month. Dell, for instance, promises to ship pre-ordered Windows 10 systems on July 29.

Mozilla Patches Critical Vulnerabilities in Firefox Update

Mozilla has issued a new Firefox browser update with fixes for four critical vulnerabilities and a number of less severe issues.

It is advised that users update their Firefox browser to the latest version, as these vulnerabilities could be exploited by cyberattackers looking to hijack sessions or steal sensitive data.

In Firefox 39, a total of four critical vulnerabilities, two high-level flaws and six moderate bugs have been patched among a total of 13 fixes. According to the Mozilla security advisory, security issues relate to use-after-free vulnerabilities, poor validation processes, buffer overflow problems and a variety of memory problems.

Two of the most critical issues are use-after-free vulnerabilities. When using XMLHttpRequest, an API used by the Firefox browser to request data from a server, in concert with either shared or dedicated workers, errors occur when the XMLHttpRequest object is attached to a worker - but that object is incorrectly deleted while still in use. This, in turn, can lead to exploitable crashes.

In addition, seven vulnerabilities, lumped together under one critical bug advisory, relate to released browser code. Three vulnerabilities were discovered as uses of uninitialized memory, one related to poor validation leading to an exploitable crash, one read of unowned memory in .zip files, and two issues led to buffer overflows.

Separately, these bugs could not be exploited easily through web content, but according to Mozilla "are vulnerable if a mechanism can be found to trigger them."

Another critical vulnerability is a use-after-free flaw which occurs when a Content Policy modifies the Document Object Model to remove a DOM object. An error in microtask implementation can lead to an exploitable browser crash - however, this flaw cannot generally be exploited through

Thunderbird email because scripting is disabled.

The last critical vulnerability relates to memory safety bugs in the browser engine. Mozilla says a number of bugs could corrupt memory "under certain circumstances," and may be exploited to run arbitrary code.

Other bugs fixed include signature validation errors, privilege escalation flaws, ServerKeyExchange skipping bugs and type confusion problems.

Chrome Continues To Trounce Firefox in Desktop Browser Market

Firefox continues to lag behind Chome in Web traffic. Net Applications Google’s Chrome keeps gaining in popularity over rival Firefox, which has failed to garner much in the way of users as seen in Web traffic numbers recorded by Net applications.

For the month of June, Chrome’s share of Web traffic across the world rose to 27.2 percent from 26.3 percent in May, 25.6 in April and 24.9 in March. During the past year, Chrome’s share has shown a significant rise from the 19.3 percent in June 2014.

Firefox’s ride has been less cheerful. In June, Mozilla’s browser grabbed a Web traffic share of 12 percent, up slightly from 11.8 percent in May and 11.7 percent in April. Over time, though, Firefox’s share has actually fallen. Its June 2014 share of Web traffic was 15.5 percent, according to Net Applications.

Why the rise for Chrome? Google’s browser has long been considered cleaner and less bloated than Microsoft’s Internet Explorer and even Mozilla’s Firefox. By default, Chrome eschews menu bars, toolbars and other items that chew up valuable screen real estate. Mozilla has tried to follow the trend of a less bloated browser with its most recent releases, yet Chrome continues to edge up in the ratings as Google keeps fine-tuning its browser. Chrome also offers quicker access to Gmail, built-in language translation, integration with Chrome apps and other features that likely appeal to Google users.

And what of Microsoft’s Internet Explorer?

IE is still at the top of the pack, with a 58.1 percent share of Web traffic for June, up slightly from 57.8 in May. Over time, IE’s share has been relatively flat, according to Net Applications, as the real battle has been between Chrome and Firefox. But despite its dominant market share, IE is getting long in the tooth and even Microsoft seems to be losing faith in it. The Windows 10 operating system, which arrives for consumers at the end of July, will offer an alternative browser called Edge.

Designed to be sleeker, faster and less burdened by add-ons and extensions, Edge is being touted by Microsoft as one of the draws for Windows 10. Oh, Internet Explorer will still be around in Windows 10, and will probably still hang onto a hefty number of users. But it although it has been getting a cleaner, more streamlined look in recent updates, IE could use a good overhaul at this point if Microsoft still wants to keep it relevant.

Among specific browser versions, Internet Explorer 11 was tops last month

with a Web traffic share of 27 percent, followed by Chrome version 43 with 17.5 percent and the aging IE 8 with 13.5 percent.

Net Applications' stats differ from those of other Web trackers. StatCounter, for example, has long shown Chrome dominating over IE, Firefox and the rest of the pack in Web traffic. Why the difference? Each Web tracker uses its own somewhat unique methods and sources to determine Web traffic data. For example, Net Applications counts unique visitors per day rather than page views and has a stronger presence in certain countries than do other Web trackers.

DuckDuckGo Search Traffic Soars 600% Post-Snowden

When Gabriel Weinberg launched a new search engine in 2008 I doubt even he thought it would gain any traction in an online world dominated by Google.

Now, seven years on, Philadelphia-based startup DuckDuckGo - a search engine that launched with a promise to respect user privacy - has seen a massive increase in traffic, thanks largely to ex-NSA contractor Edward Snowden's revelations.

Since Snowden began dumping documents two years ago, DuckDuckGo has seen a 600% increase in traffic (but not in China - just like its larger brethren, its blocked there), thanks largely to its unique selling point of not recording any information about its users or their previous searches.

Such a huge rise in traffic means DuckDuckGo now handles around 3 billion searches per year.

Speaking on CNBC, CEO Gabriel Weinberg explained how mainstream search engines make money by tracking their customers around the web, saying "It's really a myth that you need to track people to make money in search," adding that DuckDuckGo makes its money by keyword advertising: "You type in car and you get a car ad. And it's really that straight forward".

By way of comparison, Weinberg said:

Google tracks you on all of these other sites because they run huge advertising networks and other properties like Gmail and photos... so they need that search engine data to track you. That's why ads follow you round the internet.

Weinberg said that by focusing purely on web search - advertisers continue to bid on lucrative keywords such as cars and mortgages - DuckDuckGo could do away with the need to track its users to turn a profit, adding that:

What consumers don't really understand is that their data is being leaked for other reasons they don't even realise.

When asked how use of DuckDuckGo differs from using Chrome's incognito mode, or other browser privacy functions, Weinberg explained how web users often misunderstood the functionality of such features:

This is another big myth people have. Incognito mode actually is only for

your computer and not around the internet. So when you're in incognito mode Google is still tracking you, your ISP still knows where you're going. All the sites you visit can still track you, including advertisers.

Mozilla decided to add DuckDuckGo as a pre-installed search engine choice in Firefox last year, and it has been included in Apple's list of search engine providers since iOS 8 and OS X 10.10.

Recent research suggests that 40% of Americans would prefer to use a search engine that does not track their internet activity, and Weinberg believes that indicates huge market potential for the company.

He did, however, concede that brand awareness was an issue, saying that "Our main issue is just that no-one has heard of us".

When it was put to Weinberg that it would make a big difference to consumers if they knew what information was out there about them, who has it, and how they could control it, he said:

People want transparency, they want to know what's going on, they want control so they can opt out and unfortunately they're usually getting neither today. We're offering some real choice.

Poisoning Google Search Results and Getting Away With It

SophosLabs researchers recently uncovered a hack being used by unscrupulous web marketers to trick Google's page ranking system into giving them top billing, despite Google's ongoing efforts to thwart this sort of search poisoning.

Over on the Sophos Blog, technical expert Dmitry Samosseiko explains how the scammers did it, and how SophosLabs spotted what they were up to.

Here on Naked Security, we decided to take a look at why search engine poisoning matters, and what we can do as a community if we see that something is not what it seems.

Put your hand up (literally, if you like) if you have ever done either or both of these:

Set out to research a topic or a product thoroughly. Used your favourite search engine. Then gone no further than the first couple of results on the very first page. Job done.

Used a search engine to gauge whether a business or website has been around a while and built up trust in that time. Seen it near the top of the first page of results. Job done.

If you have, you aren't alone, and that's why doing well in search results is so important for a modern organisation.

And that, in turn, is why Search Engine Optimisation (SEO) exists: you make every effort to write your web pages so they are clear and relevant, and you do your best to build up a reputation that makes already-trusted sites want to link to you.

When others link to you, that acts as an implicit recommendation, and

search engines let you bask in some of the reflected glory of the sites that have linked to you.

Of course, getting high up in the search rankings gives great results for cybercrooks too, and they don’t play by the rules.

Treachery by cybercrooks gives search companies a double whammy: the search engines end up not only giving away artificially high rankings for free, but also conferring trust even on web pages that put users in harm’s way.

As a result, the search companies have been in a constant battle with the Bad Guys to stamp out tricks that poison search rankings.

One search poisoning technique involves being two-faced: looking honest and reputable when a search engine visits in the course of indexing the web, yet serving up malevolent content when a user clicks through.

This trick is called cloaking, and it’s been going on for years.

As you can imagine, the search engines have become adept at detecting when websites feed back content that doesn’t look right.

For example, they can compare what happens when their own search engine software (known as a spider or a crawler) comes calling, and what shows up when a regular browser visits the site.

Servers often tweak the pages they present depending on which browser you’re using, so some variation between visits is to be expected.

But if a browser sees a story about apples while the crawler is being sold on oranges, then something fishy is probably going on.

Additionally, a search engine can analyse the pages that its crawler finds in order to estimate how realistic they look.

Google’s crawler is known officially, as you see in the HTTP header example above as the Googlebot, and it has been taught to be rightly suspicious of web pages that seem to "try too hard" because they’ve been artificially packed with fraudulent keywords.

But even Google doesn’t get it right all the time.

Indeed, SophosLabs recently spotted dodgy web marketers using a surprisingly simple trick to persuade the usually-sceptical Googlebot to accept bogus content.

The trick inflated the reputation of dubious pages, and sent them dishonestly scooting up the search rankings.

Our researchers immediately informed Google so that the problem could be fixed, but the story makes for fascinating reading.

Dmitry Samosseiko of SophosLabs has published a highly readable report about what happened; we’re not going to spoil the fun by repeating it here, so please head over to our Sophos Blog for the details.

If you see something suspicious, such as web pages that don’t match what you searched for, or emails that link where you don’t expect, say something!

You can report suspicious emails, web pages and files to Sophos:

By email, but please read our instructions so we receive the content in a form we can use.

Via our web submission system.

And, remember, don't treat a few top-ranking search results as a replacement for due diligence when you're trying to learn more about a company or a product especially a software product that you're thinking of downloading.

Search engines can have their moments of gullibility, too!

=~=~=~=